

MILNOR K -THEORY AND THE GRADED REPRESENTATION RING

PIERRE GUILLOT AND JÁN MINÁČ

ABSTRACT. Let F be a field, let $G = \text{Gal}(\bar{F}/F)$ be its absolute Galois group, and let $R(G, \mathbf{k})$ be the representation ring of G over a suitable field \mathbf{k} . In this preprint we construct a ring homomorphism from the mod 2 Milnor K -theory $k_*(F)$ to the graded ring $\text{gr } R(G, \mathbf{k})$ associated to Grothendieck's γ -filtration. We study this map in particular cases, as well as a related map involving the W -group \mathcal{G} of F , rather than G . The latter is an isomorphism in all cases considered.

Naturally this echoes the Milnor conjecture (now a theorem), which states that $k_*(F)$ is isomorphic to the mod 2 cohomology of the absolute Galois group G , and to the graded Witt ring $\text{gr } W(F)$.

The machinery developed to obtain the above results seems to have independent interest in algebraic topology. We are led to construct an analog of the classical Chern character, which does not involve complex vector bundles and Chern classes but rather real vector bundles and Stiefel-Whitney classes. Thus we show the existence of a ring homomorphism whose source is the graded ring associated to the real K -theory ring $K(X)$ of the topological space X , again with respect to the γ -filtration, and whose target is a certain subquotient of $H^*(X, \mathbf{F}_2)$.

In order to define this subquotient, we introduce a collection of distinguished Steenrod operations. They are related to Stiefel-Whitney classes by combinatorial identities.

1. INTRODUCTION

The Milnor conjecture ([Mil70]), now a theorem by Voevodsky ([Voe03b] and [Voe03a]), is the statement that a certain map

$$h_F: k_*(F) \longrightarrow H^*(F, \mathbf{F}_2)$$

is an isomorphism. Here we have written $k_*(F)$ for mod 2 Milnor K -theory, and $H^*(F, \mathbf{F}_2)$ for the Galois cohomology of F (that is, the cohomology of its absolute Galois group). However, the conjecture has a second part, proved by Orlov, Vishik and Voevodsky ([OVV07]), according to which there is also an isomorphism

$$s: k_*(F) \longrightarrow \text{gr } W(F),$$

where $W(F)$ is the Witt ring of F , and where $\text{gr } W(F)$ denotes the graded ring associated to the filtration by powers of the fundamental ideal I . In his original paper Milnor relates these two statements by means of a commutative square:

$$\begin{array}{ccc} k_n(F) & \xrightarrow{s} & \text{gr}^n W(F) = I^n/I^{n+1} \\ h_F \downarrow & & \downarrow w_{2^{n-1}} \\ H^n(F, \mathbf{F}_2) & \xrightarrow{\times \ell(-1)^{t-n}} & H^{2^{n-1}}(F, \mathbf{F}_2). \end{array}$$

Here $\ell(-1)$ is a certain distinguished element in Galois cohomology, and the bottom map is multiplication by $\ell(-1)^{t-n}$ where $t = 2^{n-1}$; the map denoted by $w_{2^{n-1}}$ is (an algebraic variant of) a Stiefel-Whitney class. This shows for example that,

whenever h_F is injective and $\ell(-1)$ is not a zero divisor, then s is also injective (see Theorem 4.1 and Remark 4.2 in [Mil70]).

The map $w_{2^{n-1}}$ is *a priori* not part of a *ring* homomorphisms from $\text{gr } W(F)$ into the cohomology ring. However, one may at least put (writing $|x|$ for the degree of x):

$$\mathfrak{I}_F = \{x \in H^*(F, \mathbf{F}_2) : \ell(-1)^{2^{|x|-1}-|x|} x = 0\}.$$

It is clear that \mathfrak{I}_F is an ideal in $H^*(F, \mathbf{F}_2)$, and thus one gets a commutative square of maps of rings:

$$\begin{array}{ccc} k_*(F) & \xrightarrow{s} & \text{gr } W(F) \\ h_F \downarrow & & \downarrow \\ H^*(F, \mathbf{F}_2) & \longrightarrow & H^*(F, \mathbf{F}_2)/\mathfrak{I}_F. \end{array}$$

Motivated by this, and with a view towards an application in field theory, the first question we adress in the paper is one in algebraic topology: given a topological space X , is there always an ideal \mathfrak{I}_X within the cohomology $H^*(X, \mathbf{F}_2)$ which generalizes the ideal \mathfrak{I}_F in the case of fields? Before we state the (positive) answer, we need to present another crucial player in this game, which is to replace the Witt ring. Namely, we shall consider the real K -theory of X , written $K(X)$, and the so-called γ -filtration: this is defined *via* a general construction, due to Grothendieck, which applies to any λ -ring (see [AT69], [FL85]). Our result, involving the associated graded ring $\text{gr } K(X)$ with respect to this filtration, is the following.

THEOREM 1.1 – *There is a collection of Steenrod operations θ_n , for $n \geq 1$, each of degree $2^{n-1} - n$, with the following properties. For any topological space X , let $\mathcal{W}^*(X)$ be the subring of $H^*(X, \mathbf{F}_2)$ generated by the Stiefel-Whitney classes of real vector bundles over X . If we put*

$$\mathfrak{I}_X = \{x \in \mathcal{W}^*(X) : \theta_{|x|} x = 0\},$$

then \mathfrak{I}_X is an ideal in $\mathcal{W}^(X)$.*

Moreover, there is an explicit map of graded rings

$$\omega : \text{gr } K(X) \longrightarrow \mathcal{W}^*(X)/\mathfrak{I}_X.$$

In the text, this consists of Corollary 2.8 and Theorem 3.6; in Lemma 4.5, we eventually prove that \mathfrak{I}_X is indeed a generalization of \mathfrak{I}_F .

We think of the map ω as a analog of the classical Chern character. It is worth pointing out that its construction involves, in degree n , the map $w_{2^{n-1}}$ as above. To give a flavour of the operations θ_n , let us indicate that $\theta_1 = \theta_2 = 1$,

$$\begin{aligned} \theta_3 &= Sq^1, & \theta_4 &= Sq^3 Sq^1 + Sq^4, & \theta_5 &= Sq^7 Sq^3 Sq^1 + Sq^8 Sq^2 Sq^1, \\ \theta_6 &= Sq^{15} Sq^7 Sq^3 Sq^1 + Sq^{16} Sq^6 Sq^3 Sq^1 + Sq^{16} Sq^7 Sq^3 + Sq^{16} Sq^8 Sq^2, \end{aligned}$$

and

$$\begin{aligned} \theta_7 &= Sq^{31} Sq^{15} Sq^7 Sq^3 Sq^1 + Sq^{32} Sq^{14} Sq^7 Sq^3 Sq^1 \\ &\quad + Sq^{32} Sq^{15} Sq^7 Sq^2 Sq^1 + Sq^{32} Sq^{16} Sq^6 Sq^2 Sq^1 + Sq^{32} Sq^{16} Sq^8 Sq^1. \end{aligned}$$

We will compute the ideal in many cases, mostly for classifying spaces of finite groups. We also treat the universal case of the space $(BO_\infty)^N$, which produces relations in \mathfrak{I}_X for any space X easily. In all of our examples we have $\mathcal{W}^*(X) = H^*(X, \mathbf{F}_2)$ (as is often the case with familiar spaces).

This Theorem finds the following purely algebraic applications. An important example of λ -ring is given by the representation ring $R(G, \mathbf{k})$ of the finite group G over the field \mathbf{k} . One may go through Grothendieck's construction of the γ -filtration in this case, and consider again the graded ring $\text{gr } R(G, \mathbf{k})$. Few results are available

about these, and the reason may be that the early investigations of the γ -filtration on a λ -ring K were strongly focused on $K \otimes \mathbf{Q}$; indeed under some conditions one has an isomorphism $K \otimes \mathbf{Q} \cong \text{gr } K \otimes \mathbf{Q}$, one of the highlights of the theory (for example see Theorem III 3.5 in [FL85]). By contrast, each graded piece $\text{gr}^n R(G, \mathbf{k})$ is torsion when G is finite ($n \geq 1$), so that the ring $\text{gr } R(G, \mathbf{k}) \otimes \mathbf{Q}$ is not interesting.

After giving some elementary calculations, namely in the case when G is cyclic and \mathbf{k} is either algebraically closed or $\mathbf{k} = \mathbf{R}$, we achieve the computation of $\text{gr } R(G, \mathbf{k}) \otimes \mathbf{F}_2$ when G is an elementary abelian 2-group. This relies heavily on the map ω , and indeed we are not aware of any other approach. More precisely, we use the map

$$R(G, \mathbf{R}) \longrightarrow K(BG),$$

obtained by associating to any representation $r: G \rightarrow O_n$ the vector bundle whose classifying map is $Br: BG \rightarrow BO_n$; this is a homomorphism of λ -rings, so it is compatible with the γ -filtration and induces a homomorphism between the associated graded rings. Combined with ω , this yields a useful map $\text{gr } R(G, \mathbf{R}) \rightarrow \mathcal{W}^*(BG)/\mathcal{I}_{BG}$. When G is elementary abelian, it is an isomorphism, though this is far from being always true.

Based on this, one can tackle many groups of small size, by considering their elementary abelian subgroups, and in this fashion we compute $\text{gr } R(D_4, \mathbf{k}) \otimes \mathbf{F}_2$, where D_4 is the dihedral group of order 8.

As our final topic, we return to Milnor's conjecture and propose a variant. The following Theorem gave its name to this paper.

THEOREM 1.2 – *Let F be any field, and let \mathbf{k} be any field of characteristic different from 2, not containing $\sqrt{-1}$. Let \bar{F} be the separable closure of F , and let $G = \text{Gal}(\bar{F}/F)$ be the absolute Galois group of F . Then there is a map*

$$\rho: k_*(F) \longrightarrow \text{gr } R(G, \mathbf{k}) \otimes \mathbf{F}_2.$$

If \mathbf{k} possesses an embedding into \mathbf{R} , then there is a commutative square

$$\begin{array}{ccc} k_*(F) & \xrightarrow{\rho} & \text{gr } R(G, \mathbf{k}) \otimes \mathbf{F}_2 \\ h_F \downarrow & & \downarrow \omega \\ H^*(F) & \longrightarrow & H^*(F)/\mathcal{I}_F. \end{array}$$

If moreover F also has characteristic $\neq 2$, and if we call \mathcal{G} the W -group of F , then there is a map

$$\rho: k_*(F) \longrightarrow (\text{gr } R(\mathcal{G}, \mathbf{k}) \otimes \mathbf{F}_2)_{dec}.$$

And if \mathbf{k} possesses an embedding into \mathbf{R} , then there is a commutative square

$$\begin{array}{ccc} k_*(F) & \xrightarrow{\rho} & (\text{gr } R(\mathcal{G}, \mathbf{k}) \otimes \mathbf{F}_2)_{dec} \\ h_F \downarrow & & \downarrow \omega \\ H^*(\mathcal{G})_{dec} & \longrightarrow & H^*(\mathcal{G})_{dec}/\mathcal{I}_{\mathcal{G}}. \end{array}$$

Recall that the W -group of a field is a certain quotient \mathcal{G} of the Galois group G , which is frequently much easier to study. Also, we use the notation A_{dec}^* for the *decomposable part* of the graded algebra A^* , that is, the subalgebra generated by elements of degree 1. For example one has famously

$$H^*(G, \mathbf{F}_2) = H^*(\mathcal{G}, \mathbf{F}_2)_{dec}.$$

The proof of this Theorem relies on an understanding of the rings $\text{gr } R(D_4, \mathbf{k})$ and $\text{gr } R(\mathbf{Z}/4, \mathbf{k})$. Moreover, the computations we perform with $\text{gr } R(G, \mathbf{k})$ throughout

the article are useful for studying the map ρ on examples. We end up proving that the map

$$k_*(F) \xrightarrow{\rho} (\mathrm{gr} R(\mathcal{G}, \mathbf{R}) \otimes \mathbf{F}_2)_{dec}$$

is an isomorphism when F is a finite field, or a local field, or a real-closed field, or a global field, or when $\ell(-1)$ is not a zero divisor in $H^*(F, \mathbf{F}_2)$, and in several other cases. There is no example yet for which this map is not an isomorphism. (This would also hold with $\mathbf{k} = \mathbf{Q}$ instead of $\mathbf{k} = \mathbf{R}$, and we shall argue that there is essentially no other interesting choice for \mathbf{k}).

The paper is organized as follows. In Section 2, we present the operations θ_n and use them to define the ideal \mathfrak{I}_X . In Section 3, we construct the “character” ω ; we also use our new machinery in order to compute the ring $\mathrm{gr} R(G, \mathbf{k})$ for several examples of finite groups G . Finally in Section 4, we return to Milnor K -theory and define the map ρ .

Acknowledgements. The first-named author would like to thank the Pacific Institute for Mathematical Sciences at Vancouver for its warm welcome during the year 2010-2011, and the Centre National de la Recherche Scientifique in France for the financial support that made this visit possible. Both authors thank Sunil Chebolu for stimulating discussions.

2. THE CANONICAL IDEAL

In this section we prove that the mod 2 cohomology of any topological space possesses a canonical subquotient. The latter will be the target of a map from the graded K -theory ring, as described in the next section. Proofs are mainly combinatorial.

2.1. The operations θ_n . The *real* topological K -theory of the topological space X will be denoted by $K(X)$. The mod 2 cohomology of the same space we write $H^*(X)$.

Given a class $t \in H^1(X) = [X, \mathbf{R}\mathbb{P}^\infty]$, one can consider the corresponding line bundle L over X . The first Stiefel-Whitney class of L , essentially by definition, is $w_1(L) = t$. Our first objective is to study an analogous relationship between line bundles and Stiefel-Whitney classes, as follows.

THEOREM 2.1 – *For each $n \geq 1$, there is a Steenrod operation θ_n with the following property. Given a space X and classes $t_1, t_2, \dots, t_n \in H^1(X)$, let L_i be the line bundle corresponding to t_i . Let ρ denote the virtual vector bundle over X defined by*

$$\rho = (L_1 - 1)(L_2 - 1) \cdots (L_n - 1),$$

where 1 stands for the trivial line bundle. Then the Stiefel-Whitney class $w_i(\rho)$ is zero for $1 \leq i < 2^{n-1}$, while

$$w_{2^{n-1}}(\rho) = \theta_n(t_1 t_2 \cdots t_n).$$

EXAMPLE 2.2 – As $w_1(L - 1) = w_1(L) = t$ we see that we may take the identity operation for θ_1 . A quick calculation shows that the second Stiefel-Whitney class of $(L_1 - 1)(L_2 - 1)$ is $t_1 t_2$, so we may again take the identity for θ_2 . On the other hand, the fourth Stiefel-Whitney class of $(L_1 - 1)(L_2 - 1)(L_3 - 1)$ is

$$t_1^2 t_2 t_3 + t_1 t_2^2 t_3 + t_1 t_2 t_3^2 = Sq^1(t_1 t_2 t_3),$$

so that Sq^1 can be taken for θ_3 .

The proof of Theorem 2.1 will occupy the rest of this section. We start with a couple of lemmas.

LEMMA 2.3 – Let $\rho \in K(X)$, and let i be the least positive integer so that $w_i(\rho) \neq 0$. Then i is a power of two.

This is well-known, and follows from Wu's formula (see [MS74]).

LEMMA 2.4 – Let $\rho \in K(X)$, and suppose that we may write $\rho = E^+ - E^-$, where E^+ and E^- are vector bundles of the same rank. Suppose also that $w_i(\rho) = 0$ for $1 \leq i < 2^{n-1}$. Then for any line bundle L , we have $w_i(\rho(L-1)) = 0$ for $1 \leq i < 2^n$.

Proof. From the previous lemma, it is enough to prove that $w_i(\rho(L-1)) = 0$ for $1 \leq i \leq 2^{n-1}$.

Here and elsewhere we shall use the total Stiefel-Whitney class, which is the homomorphism

$$w_T: K(X) \rightarrow 1 + TH^*(X)[[T]]$$

defined by $w_T(\rho) = 1 + w_1(\rho)T + w_2(\rho)T^2 + \dots$. For example, when ρ is as in the statement of the Lemma, we have $w_T(\rho) = w_T(E^+)w_T(E^-)^{-1}$, and from this we see that the hypotheses imply that

$$(*) \quad w_i(E^+) = w_i(E^-) \quad \text{for } 1 \leq i < 2^{n-1}.$$

We are interested in the Stiefel-Whitney classes of $\rho(L-1) = (LE^+ + E^-) - (LE^- + E^+)$, and thus we wish to prove that

$$(**) \quad w_i(LE^+ + E^-) = w_i(LE^- + E^+),$$

for $1 \leq i \leq 2^{n-1}$. Now, the Stiefel-Whitney classes of $LE^+ + E^-$ are given by evaluating certain universal polynomials, using the classes of L , E^+ and E^- ; moreover, these polynomials depend only on the rank of the vector bundles involved. As a result, it is clear from (*) that in degrees less than 2^{n-1} , we would obtain the same result using $LE^- + E^+$ instead. In other words, equation (**) holds for $1 \leq i < 2^{n-1}$, and the only non-trivial calculation happens for $i = 2^{n-1}$.

In this degree, we have

$$w_{2^{n-1}}(LE^+ + E^-) = w_{2^{n-1}}(LE^+) + w_{2^{n-1}}(E^-) + R_{\pm},$$

where the last term is

$$R_{\pm} = \sum_{p+q=2^{n-1}} w_p(LE^+)w_q(E^-).$$

In this sum the indices p and q are positive; arguing as above, we see that $R_{\pm} = R_{\mp}$, where R_{\mp} is defined by exchanging E^+ and E^- , that is

$$w_{2^{n-1}}(LE^- + E^+) = w_{2^{n-1}}(LE^-) + w_{2^{n-1}}(E^+) + R_{\mp}.$$

The Lemma will be proved if we can establish that $w_{2^{n-1}}(LE^+) + w_{2^{n-1}}(E^-) = w_{2^{n-1}}(LE^-) + w_{2^{n-1}}(E^+)$.

Let $a = w_1(L)$. Then the 2^{n-1} -st Stiefel-Whitney class of LE^+ is given by

$$w_{2^{n-1}}(LE^+) = a^{2^{n-1}} + w_1(E^+)a^{2^{n-1}-1} + w_2(E^+)a^{2^{n-1}-2} + \dots + w_{2^{n-1}}(E^+).$$

So, using (*) again, we see indeed that $w_{2^{n-1}}(LE^+) + w_{2^{n-1}}(E^-)$ is left unchanged when E^+ and E^- are exchanged. This concludes the proof. \square

This Lemma gives us at once the easy part of Theorem 2.1: namely, proving that $w_i(\rho) = 0$ for $1 \leq i < 2^{n-1}$ is now achieved with a routine induction.

To go further, let us write σ_k for the k -th symmetric function in L_1, \dots, L_n , computed in the ring $K(X)$. We also write $\sigma_0 = 1$, the trivial line bundle, and we understand that $\sigma_k = 0$ for $k > n$. Put

$$E^{even} = \sum_{k \text{ even}} \sigma_k \quad \text{and} \quad E^{odd} = \sum_{k \text{ odd}} \sigma_k.$$

The virtual bundle ρ as in the statement of the Theorem is then

$$\rho = (-1)^n (E^{\text{even}} - E^{\text{odd}}).$$

We have already established that $w_i(E^{\text{even}}) = w_i(E^{\text{odd}})$ for $1 \leq i < 2^{n-1}$. Note that E^{even} and E^{odd} both have rank 2^{n-1} , and that E^{even} contains a copy of the trivial line bundle σ_0 ; as a result, we finally have $w_{2^{n-1}}(\rho) = w_{2^{n-1}}(E^{\text{odd}})$.

We can make this quite explicit. Indeed, if we put

$$m_k = \prod_{1 \leq i_1 < i_2 < \dots < i_k \leq n} (t_{i_1} + t_{i_2} + \dots + t_{i_k}),$$

then it is readily seen that

$$w_{2^{n-1}}(E^{\text{odd}}) = \prod_{k \text{ odd}} m_k.$$

The following Lemma gives an expansion of the right hand side. It is crucial to the proof of the Theorem, and indeed can be considered to lie at the core of the paper.

LEMMA 2.5 – *In the polynomial ring $\mathbf{F}_2[t_1, \dots, t_n]$, one has the following identity:*

$$\prod_{k \text{ odd}} m_k = \sum_{2^{r_1} + \dots + 2^{r_n} = 2^{n-1}} t_1^{2^{r_1}} t_2^{2^{r_2}} \dots t_n^{2^{r_n}}.$$

For example for $n = 3$ this gives

$$t_1 t_2 t_3 (t_1 + t_2 + t_3) = t_1^2 t_2 t_3 + t_1 t_2^2 t_3 + t_1 t_2 t_3^2.$$

Proof. Let P denote the polynomial on the right hand side, given as a sum. We write $P(t_1 \leftarrow t_i)$ for $P(t_i, t_2, t_3, \dots, t_n)$.

Consider a fixed term of the sum defining $P(t_1 \leftarrow t_i)$. If $r_1 \neq r_i$, then the sum will contain another term with r_1 and r_i swapped; but this will be the same term because $t_1 = t_i$ now, so they will cancel. The only terms remaining, for $r_1 = r_i$, will add up to

$$\sum_{\substack{2^{r_2} + \dots + 2^{r_n} = 2^{n-1} \\ r_i \geq 1}} t_2^{2^{r_2}} \dots t_n^{2^{r_n}}.$$

The reason for $r_i \geq 1$ is that 2^{r_i} has really absorbed $2^{r_1} + 2^{r_i} = 2 \cdot 2^{r_i} = 2^{r_i+1}$. However, here is an elementary observation: $2^{n-1} - 1$ cannot be written as the sum of $n - 2$ powers of 2. It follows that the condition $r_i \geq 1$ is in fact automatically satisfied (otherwise $2^{r_i} = 1$ and we have written $1 + 2^{r_2} + \dots + 2^{r_n} = 2^{n-1}$ which is impossible). Erase the condition $r_i \geq 1$ in the sum above: the result now blatantly is independent of i . So $P(t_1 \leftarrow t_i) = P(t_1 \leftarrow t_j)$, for any pair of indices i, j .

In particular, we see that

$$P(t_1 \leftarrow t_i + t_j) = P(t_1 \leftarrow t_i) + P(t_1 \leftarrow t_j) = 0.$$

As a result the polynomial P is divisible by $(t_1 + t_i + t_j)$. Of course the variable t_1 can be replaced by any other, and likewise we see that P is divisible by $(t_i + t_j + t_k)$ for any triple (i, j, k) . It is also easy to continue, for example

$$P(t_1 \leftarrow t_{i_1} + t_{i_2} + t_{i_3} + t_{i_4}) = P(t_1 \leftarrow t_{i_1} + t_{i_2}) + P(t_1 \leftarrow t_{i_3} + t_{i_4}) = 0 + 0 = 0,$$

so P is divisible by $(t_1 + t_{i_1} + t_{i_2} + t_{i_3} + t_{i_4})$. Pursuing the calculations in this fashion, we see that P is divisible by all the terms of m_k as long as k is odd. These terms are coprime in the ring $\mathbf{F}_2[t_1, \dots, t_n]$, so P is divisible by their product, and a comparison of the degrees gives the result. \square

We can finally describe θ_n . We are going to rely on Milnor's description of the dual \mathcal{A}^* of the Steenrod algebra, see [Mil58]. Recall that

- (1) \mathcal{A}^* is polynomial on variables ζ_i in degree $2^i - 1$.
- (2) For any space X , there is a map *of rings*

$$\lambda^*: H^*(X) \rightarrow H^*(X) \otimes \mathcal{A}^*,$$

such that, for any Steenrod operation θ and element $x \in H^*X$, we can recover θx by evaluating $\lambda^*(x)$ at θ .

- (3) For $X = B\mathbf{Z}/2$, whose cohomology is $\mathbf{F}[t]$, one has

$$\lambda^*(t) = \sum t^{2^i} \otimes \zeta_i.$$

This allows the computation of $\lambda^*(t_1 \cdots t_n)$ in our situation. If we define

$$Sq(i_1, i_2, \dots, i_k)$$

to be the Steenrod operation dual to $\zeta_1^{i_1} \cdots \zeta_k^{i_k}$, we may put

$$\theta_n = \sum Sq(i_1, \dots, i_k)$$

where the sum runs over all the elements which have degree $2^{n-1} - n$. We have then $\theta_n(t_1 \cdots t_n) = P$, where P is again the right-hand side in the identity of Lemma 2.5. This Lemma thus asserts that

$$\theta_n(t_1 \cdots t_n) = w_{2^{n-1}}(\rho),$$

which concludes the proof of Theorem 2.1.

Remark 2.6. The reader may compute θ_n easily using the free computer algebra system SAGE, simply by entering

```
theta= lambda n: sum(SteenrodAlgebra(2,"milnor").basis(2^(n-1)-n)).basis("serre-cartan")
```

Subsequent calls to `theta(n)` will give the value of θ_n , in terms of the Sq^k 's. The examples given in the Introduction were computed in this way.

2.2. The ideal. Given any graded algebra A^* , we write A_{dec}^* for the subalgebra generated by the elements of degree 1.

PROPOSITION 2.7 – *For any topological space X , let us put*

$$I_{dec} = \{x \in H^*(X)_{dec} : \theta_{|x|}(x) = 0\}.$$

Then I_{dec} is an ideal in $H^(X)_{dec}$.*

Here $|x|$ is the degree of x .

Proof. Let $n = |x|$, and assume that $\theta_n(x) = 0$. It is enough to prove that, for y of degree 1, we have $\theta_{n+1}(xy) = 0$.

The element x is a sum of products of n elements of degree 1, and by applying Theorem 2.1 several times, we see that there exists some virtual vector bundle ρ over X such that $\theta_n(x) = w_{2^{n-1}}(\rho)$, while $w_i(\rho) = 0$ for $1 \leq i < 2^{n-1}$. Here we rely on the observation that, if ρ_1 and ρ_2 are vector bundles such that the Stiefel-Whitney classes of *both* ρ_1 and ρ_2 vanish in degrees less than 2^{n-1} , then the same can be said of the sum $\rho_1 + \rho_2$, and moreover $w_{2^{n-1}}(\rho_1 + \rho_2) = w_{2^{n-1}}(\rho_1) + w_{2^{n-1}}(\rho_2)$. Our assumption on x implies thus that $w_{2^{n-1}}(\rho) = 0$, so that, by Lemma 2.3, we have actually $w_i(\rho) = 0$ for $1 \leq i < 2^n$.

A similar reasoning with xy shows that $\theta_{n+1}(xy) = w_{2^n}(\rho(L-1))$, where L is the line bundle defined by y . Lemma 2.4 guarantees that this Stiefel-Whitney class vanishes, thus establishing the Proposition. \square

We can make a stronger statement using the “splitting principle”. This classical result states that, given a finite number of vector bundles E_1, \dots, E_k over X , one can find a space Y with a map $p: Y \rightarrow X$, such that

(1) the map $p^*: H^*(X) \rightarrow H^*(Y)$ is injective, and

(2) each of E_1, \dots, E_k splits as a sum of line bundles, when pulled-back over Y .

In particular, the classes $p^*(w_i(E_j))$ all belong to $H^*(Y)_{dec}$. From this we obtain the following.

COROLLARY 2.8 – *Let $\mathcal{W}^*(X)$ denote the subring of $H^*(X)$ generated by Stiefel-Whitney classes. Put*

$$\mathfrak{I}_X = \{x \in \mathcal{W}^*(X) : \theta_{|x|}(x) = 0\}.$$

Then \mathfrak{I}_X is an ideal in $\mathcal{W}^(X)$.*

The canonical subquotient $\mathcal{W}^*(X)/\mathfrak{I}_X$ of $H^*(X)$ will be one of our chief interests in the rest of the paper. The following Lemma states some of its easy but useful properties.

LEMMA 2.9 – *Let $f: Y \rightarrow X$ be any map. Then*

(1) *We have $f^*(\mathcal{W}^*(X)) \subset f^*(\mathcal{W}^*(Y))$ and $f^*(\mathfrak{I}_X) \subset f^*(\mathfrak{I}_Y)$, so that there is an induced map $f^\sharp: \mathcal{W}^*(X)/\mathfrak{I}_X \rightarrow \mathcal{W}^*(Y)/\mathfrak{I}_Y$.*

(2) *If f^* is injective, so is f^\sharp .*

Proof. Property (1) is obvious given the naturality of both Stiefel-Whitney classes and Steenrod operations. We turn to (2).

Suppose that $f^\sharp(x) = 0$, so that $f^*(x) \in \mathfrak{I}_Y$. By definition, this means that $\theta_n(f^*(x)) = 0$, where n is the degree of x . However, we have then $f^*(\theta_n(x)) = 0$ so that $\theta_n(x) = 0$ by injectivity of f^* , and we see that $x \in \mathfrak{I}_X$. \square

In what follows we shall be particularly interested in the case $X = BG$, the classifying space of the group G . In this situation we will use notation such as $H^*(G)$, $\mathcal{W}^*(G)$ and \mathfrak{I}_G . Here is a first example.

PROPOSITION 2.10 – *Let $G = (\mathbf{Z}/2)^r$ be elementary abelian of rank r . Then the cohomology ring $H^*(G) = \mathcal{W}^*(G) = \mathbf{F}_2[t_1, \dots, t_r]$ is polynomial, and the ideal \mathfrak{I}_G is generated by the elements $t_i^2 t_j + t_i t_j^2$, for $1 \leq i, j \leq r$.*

Of course the statement about $H^*(G)$ is classical. We point out that an equivalent formulation of the Proposition is that \mathfrak{I}_G is generated as an ideal by the kernel of $Sq^1 = \theta_3$ viewed as a map $H^3(G) \rightarrow H^4(G)$.

Proof. We have

$$Sq^1(t_i^2 t_j + t_i t_j^2) = t_i^2 t_j^2 + t_i^2 t_j^2 = 0,$$

so certainly $t_i^2 t_j + t_i t_j^2 \in \mathfrak{I}_G$, as $\theta_3 = Sq^1$. Let J be the ideal generated by these elements, and let us prove that $\mathfrak{I}_G = J$. We have a succession of surjective maps

$$\mathbf{F}_2[t_1, \dots, t_r] \longrightarrow H^*(G)/J \longrightarrow H^*(G)/\mathfrak{I}_G.$$

Fix an integer n . It is clear that any two monomials in $H^n(G)$ are equal modulo J as soon as they are written with the same “alphabet”, ie if they involve exactly the same variables. In order to exploit this, for any non-empty subset S of $\{1, 2, \dots, r\}$ of cardinality $\leq n$ we pick a monomial $x_S \in H^n(G)$ which involves the variables t_i for $i \in S$ and no other; we also arrange so that only one variable is raised to a power greater than 1. Concretely, if $S = \{i_1, \dots, i_s\}$, we may take $x_S = t_{i_1}^{n-s+1} t_{i_2} \cdots t_{i_s}$. We have observed that the elements x_S , for such subsets S , generate $H^n(G)/J$, and we shall prove now that they are linearly independent even in $H^n(G)/\mathfrak{I}_G$. It will follow that these elements form a basis of

both $H^n(G)/J$ and $H^n(G)/\mathfrak{J}_G$, and this being true for all n , we are compelled to conclude that $\mathfrak{J}_G = J$.

Examining the definitions, we see that we must establish that the elements $\theta_n(x_S)$ are linearly independent in $H^{2^{n-1}}(G)$. So let us assume that we are given a zero linear combination, say

$$(*) \quad \sum_S \lambda_S \theta_n(x_S) = 0.$$

Fix a T , and let us prove that $\lambda_T = 0$. The identity $(*)$ takes place in a polynomial ring, so it is possible for us to set $t_i = 0$ for $i \notin T$. From Lemma 2.5, we see that x_S and $\theta_n(x_S)$ are written in the same “alphabet”, and so the new identity we obtain only involves those subsets S such that $S \subset T$. What is more, the element $\theta_n(x_T)$ is the only one whose monomials involve *all* the variables t_i for $i \in T$. It is thus clear that we have $\lambda_T \theta_n(x_T) = 0$.

It remains to prove that $\theta_n(x_T) \neq 0$. From the construction of x_T , we know that there is some variable, say t_j , which appears in x_T to the power one. Now set $t_i = 1$ for $i \in T$ if $i \neq j$ (while maintaining $t_i = 0$ for $i \notin T$), and let us prove that $\theta_n(x_T)$ is non-zero even then. Indeed, from the factorized expression for $\theta_n(x_T)$ appearing in Lemma 2.5, we know that this element is a product of terms of the form

$$m_k = (t_{i_1} + \cdots + t_{i_k})$$

where k is odd, the indices i_1, \dots, i_k are in T , and at most one of them is j . If there is no such index, then $m_k = 1$ after the variables have been set to one; if there is such an index, then $m_k = t_j$. As a result $\theta_n(x_T)$ is a power of t_j , and in particular it is not zero. It follows that $\lambda_T = 0$ and the proof is complete. \square

2.3. The universal example of BO_∞^N . We will now compute the “universal” ideal $\mathfrak{J}_N := \mathfrak{J}_{BO_\infty^N}$ for the space BO_∞^N to be described next. This will give relations in the cohomology of any space.

Consider first the classifying space BO_n of the n -th compact orthogonal group O_n ; its cohomology is

$$H^*(BO_n) = \mathbf{F}_2[w_1, w_2, \dots, w_n].$$

There are inclusions maps $O_n \rightarrow O_{n+1}$, inducing maps $BO_n \rightarrow BO_{n+1}$, and we take BO_∞ to be the colimit of this diagram. We have thus

$$H^*(BO_\infty) = \lim H^*(BO_n) = \mathbf{F}_2[w_1, w_2, w_3, \dots].$$

Here we think of w_i as a generalized Stiefel-Whitney class, and indeed Corollary 2.8 applies with $\mathcal{W}^*(BO_\infty) = H^*(BO_\infty)$, as we readily see.

Next, take an integer N and consider the cartesian product $BO_\infty^N = (BO_\infty)^N$. This space has projection maps $p_i: BO_\infty^N \rightarrow BO_\infty$, and we write $w_j(p_i)$ for the class $p_i^*(w_j)$. The cohomology of BO_∞^N is polynomial in all the classes $w_j(p_i)$, for $1 \leq i \leq N$ and $j \geq 1$. In particular $H^*(BO_\infty^N) = \mathcal{W}^*(BO_\infty^N)$ (in the same generalized sense as above).

Given any space X and vector bundles E_1, E_2, \dots, E_N over X , we have classifying maps $f_i: X \rightarrow BO_\infty$, which we may combine into a map $X \rightarrow BO_\infty^N$. The Stiefel-Whitney classes of the bundle E_i are pulled back from the classes $w_j(p_i)$, so the relations in \mathfrak{J}_N will yield relations in \mathfrak{J}_X .

Let us now state the result. It is somehow easier to give a presentation for $H^*(BO_\infty^N)/\mathfrak{J}_N$.

PROPOSITION 2.11 – *The ring $H^*(BO_\infty^N)/\mathfrak{J}_N$ is generated by the classes $w_{2j}(p_i)$, for $1 \leq i \leq N$ and $j \geq 0$. These are subject to the relations*

$$(*) \quad w_{2j_1}(p_{i_1}) \cdots w_{2j_s}(p_{i_s}) = w_{2k_1}(p_{\ell_1}) \cdots w_{2k_t}(p_{\ell_t})$$

whenever the two sides of (*) have the same degree and involve exactly the same variables.

Moreover, for any integer n , let the binary expansion of n be

$$n = \sum_{k \geq 0} a_k 2^k.$$

Then the class $w_n(p_i)$ is given in $H^*(BO_\infty^N)/\mathfrak{I}_N$ by

$$(**) \quad w_n(p_i) = \prod_{k \geq 0} w_{2^k}(p_i)^{a_k}.$$

In other words, the ideal \mathfrak{I}_N is generated by the relations (*) and (**). It follows that, for any vector bundle E over any space X whatsoever, we will always have such relations as $w_5(E) = w_1(E)w_4(E)$ modulo \mathfrak{I}_X (relation of type (**)); and if F is any other vector bundle over X , the relation $w_1(E)w_2(F)^2 = w_1(E)^3w_2(F)$ modulo \mathfrak{I}_X always holds (relation of type (*)).

Let us also state a general consequence.

COROLLARY 2.12 – *Let X be a space such that $\mathcal{W}^*(X)$ is generated by finitely many Stiefel-Whitney classes. Then there exists a constant C such that*

$$\dim_{\mathbf{F}_2} \mathcal{W}^n(X)/\mathfrak{I}_X \leq C$$

for all $n \geq 0$.

Proof of the Corollary. By the Proposition, there are no more monomials in the Stiefel-Whitney classes in a given degree than ways of picking a subset of the set of variables. \square

We turn to the proof of the Proposition. We provide details for the case $N = 1$ only, for the general case simply involves more complicated notation. Note that the cohomology of BO_∞ agrees with that of BO_m in degrees $< m$, and it will be technically easier to work with such a space BO_m with m large enough. So for the duration of this proof, the symbol ∞ will stand for a conveniently large integer.

The group O_∞ has a distinguished elementary abelian subgroup $T = (\mathbf{Z}/2)^\infty$, given by the diagonal matrices with entries ± 1 . Moreover the map

$$H^*(BO_\infty) \longrightarrow H^*T = \mathbf{F}_2[t_1, \dots, t_\infty]$$

is injective, and sends w_i to the i -th symmetric function in the variables t_1, \dots, t_∞ . From Lemma 2.9, the ideal \mathfrak{I}_N is the kernel of the map $H^*(BO_\infty) \rightarrow H^*(T)/\mathfrak{I}_T$.

The ring $H^*(T)/\mathfrak{I}_T$ is given by Proposition 2.10. We see that in degree n , it has a basis in bijection with the non-empty subsets of $\{1, 2, \dots, \infty\}$ of cardinality $\leq n$. Given such a subset I , we write $t_{I,n}$ for the corresponding element. Note that the multiplication is given by the rule

$$t_{I,n} t_{J,m} = t_{I \cup J, n+m}.$$

We also put

$$t_{i,n} = \sum_{\#I=i} t_{I,n}.$$

In this notation, the image of w_i is $t_{i,i}$. We need to work out the product of w_i and w_j , and this is *a priori* given by

$$\begin{aligned} t_{i,i} t_{j,j} &= \left(\sum_{\#I=i} t_{I,i} \right) \left(\sum_{\#J=j} t_{J,j} \right) \\ &= \sum_{\#I=i, \#J=j} t_{I \cup J, i+j} \\ &= \sum_{k \geq 1} \sum_{\#K=k} \alpha_{i,j,k} t_{K, i+j}. \end{aligned}$$

This equality defines the number $\alpha_{i,j,k}$, which is clearly the number of ways of writing a set with k elements as a union $I \cup J$, where I has i elements and J has j elements. Luckily, we are considering $\alpha_{i,j,k} \bmod 2$, and the formula above can be drastically simplified.

LEMMA 2.13 – *Given i and j , there is one and only one integer k such that $\alpha_{i,j,k}$ is odd. Moreover k is given by the following recipe. Writing the binary expansions*

$$i = \sum_{s \geq 0} a_s 2^s \quad \text{and} \quad j = \sum_{s \geq 0} b_s 2^s,$$

then k is given by

$$k = \sum_{s \geq 0} \max(a_s, b_s) 2^s.$$

This number will be written $i \text{ OR } j$.

We point out that the notation $i \text{ OR } j$ is very common in computer science; it reminds the reader that a given “bit” of $i \text{ OR } j$ is set to 1 when the corresponding bit of i is 1 *or* the corresponding bit of j is 1. The operation $i, j \mapsto i \text{ OR } j$ is commutative and associative.

Proof of Lemma 2.13. For any integer n whose binary expansion is

$$n = \sum_{s \geq 0} a_s 2^s,$$

we note

$$\text{supp}(n) = \{s : a_s \neq 0\},$$

and call it the support of n . The number $i \text{ OR } j$ is characterized as the only integer whose support is $\text{supp}(i) \cup \text{supp}(j)$.

Elementary combinatorics reveal that, when $\max(i, j) \leq k \leq i + j$, the number $\alpha_{i,j,k}$ is given by

$$\begin{aligned} \alpha_{i,j,k} &= \binom{k}{i} \binom{i}{k-j} \\ &= \binom{k}{j} \binom{j}{k-i} \\ &= \frac{k!}{(k-i)!(k-j)!(i+j-k)!}. \end{aligned}$$

(For other values of k , we have $\alpha_{i,j,k} = 0$ trivially.) Now we rely on an elementary observation, which dates back to Kummer (see [Kum75], pp 507-508):

$$\binom{n}{m} \text{ is odd} \iff \text{supp}(m) \subset \text{supp}(n).$$

It appears that $\alpha_{i,j,k}$ is odd precisely when the following two conditions are satisfied:

- (a) $\text{supp}(j) \subset \text{supp}(k)$,
- (b) $\text{supp}(k - j) \subset \text{supp}(i)$.

Note that whenever (a) holds, we have $\text{supp}(k - j) = \text{supp}(k) \setminus \text{supp}(j)$. From this it is clear that (a) and (b) together are equivalent to the condition $\text{supp}(k) = \text{supp}(i) \cup \text{supp}(j)$. \square

We now see that the following relation holds in H^*T/\mathcal{J}_T :

$$t_{i,i}t_{j,j} = t_{i \text{ OR } j, i+j}.$$

It follows that

$$w_{i_1}w_{i_2} \cdots w_{i_k} = t_{i_1 \text{ OR } i_2 \text{ OR } \cdots \text{ OR } i_k, i_1+i_2+\cdots+i_k},$$

and that

$$w_{i_1}w_{i_2} \cdots w_{i_k} = w_{j_1}w_{j_2} \cdots w_{j_\ell}$$

whenever $i_1 + \cdots + i_k = j_1 + \cdots + j_\ell$ and $i_1 \text{ OR } \cdots \text{ OR } i_k = j_1 \text{ OR } \cdots \text{ OR } j_\ell$. In particular, we have

$$w_{2^{j_1}} \cdots w_{2^{j_s}} = w_{2^{k_1}} \cdots w_{2^{k_t}}$$

whenever the degrees on both sides are equal and

$$\{2^{j_1}, \dots, 2^{j_s}\} = \{2^{k_1}, \dots, 2^{k_t}\}.$$

That is, the relations (*) hold. The relations (**) are equally clear at this point.

Let J be the ideal generated by (*) and (**). To finish the proof, we need to show that $H^*(BO_\infty^N)/J$ injects into $H^*(T)/\mathcal{J}_T$. However, this is obvious, and follows from the fact that the elements $t_{i,n}$ for different values of i are linearly independent.

3. GRADED K -THEORY & GRADED REPRESENTATION RINGS

We start this section by recalling the definition of the γ -filtration on a general λ -ring. Next we consider, as first examples, the representation rings of some finite groups. Then we prove the existence of a “character”, that is a ring homomorphism, between the graded ring associated to the real K -theory of a topological space, and the subquotient of its cohomology defined in the previous section.

3.1. Grothendieck’s construction. Let us give some recollections about the γ -filtration, which is due to Grothendieck. Details may be found in [FL85], [AT69].

The general setting is that of a λ -ring K with augmentation $\varepsilon: K \rightarrow \mathbf{Z}$ (in older terminology, λ -rings were called “special λ -rings”). So for each $n \geq 0$ there is a map $\lambda^n: K \rightarrow K$, such that for each $x \in K$ one has $\lambda^0(x) = 1$, $\lambda^1(x) = x$, and all the identities presented in the references above. The kernel of ε is denoted I and called the augmentation ideal.

The γ -operations are then defined by

$$\gamma^n(x) = \lambda^n(x + n - 1),$$

for $x \in K$. For $n \geq 1$, let Γ^n be the abelian subgroup of K generated by all elements of the form

$$\gamma^{k_1}(x_1)\gamma^{k_2}(x_2) \cdots \gamma^{k_s}(x_s) \quad \text{with} \quad \sum k_i \geq n,$$

where each x_i belongs to I . One checks that each Γ^n is an ideal in K , that $\Gamma^{n+1} \subset \Gamma^n$, and that $\Gamma^1 = I$. Writing Γ^0 for K itself, one can then consider the associated graded ring

$$\text{gr } K = \Gamma^0/\Gamma^1 \oplus \Gamma^1/\Gamma^2 \oplus \Gamma^2/\Gamma^3 \oplus \cdots,$$

where $\Gamma^0/\Gamma^1 = K/I \cong \mathbf{Z}$.

Now for $x \in K$ and $i \geq 1$ we write $c_i(x)$ for the class of $\gamma^i(x - \varepsilon(x))$ in Γ^i/Γ^{i+1} . The properties of the operations λ^i on K imply the simple statement that those classes $c_i(x)$ satisfy all the familiar axioms of *Chern classes*; and indeed we shall call

them the algebraic Chern classes. This may be the place to point out that, in spite of the many references to algebraic topology in this paper, *we will never mention the topological Chern classes*, and a notation such as $c_i(x)$ is always understood in the graded ring associated to a λ -ring.

The typical example of λ -ring for us will be the real topological K -theory of a topological space on the one hand, and the representation ring $R(G, \mathbf{k})$ of a finite group G over a field \mathbf{k} on the other hand. When $\mathbf{k} = \mathbf{R}$, we note that a real representation of G defines a real vector bundle over the classifying space BG , thus yielding a map of λ -rings

$$R(G, \mathbf{R}) \longrightarrow K(BG),$$

which in turn induces a map

$$\mathrm{gr} R(G, \mathbf{R}) \longrightarrow \mathrm{gr} K(BG).$$

3.2. Elementary examples. It is our intention to advertise the rings $\mathrm{gr} R(G, \mathbf{k})$, and encourage further investigations by our readers. Computations with these have a cohomological flavour, although the results are interestingly different. Let us start with a couple of general statements.

LEMMA 3.1 – *Let G be a finite group. Then the group $\mathrm{gr}^1 R(G, \mathbf{k})$ is isomorphic to the group of 1-dimensional representations of G over \mathbf{k} , under the tensor product operation. Moreover the isomorphism is given by the first Chern class.*

Proof. This follows from Theorem 1.7, Chapter III, in [FL85]. \square

LEMMA 3.2 – *Let G be finite. Then for $n \geq 1$, the group $\mathrm{gr}^n R(G, \mathbf{k})$ is torsion. More precisely, if the order of G is $|G|$, then $\mathrm{gr}^n R(G, \mathbf{k})$ is killed by $|G|^n$.*

Thus the ring $\mathrm{gr} R(G, \mathbf{k}) \otimes \mathbf{Q}$ is isomorphic to \mathbf{Q} concentrated in degree 0. The early investigations of the Grothendieck filtration focused on $\mathrm{gr} K \otimes \mathbf{Q}$ (in particular in the case when $K = K(X)$, the K -theory of an algebraic variety), which the Lemma shows is not interesting for $K = \mathrm{gr} R(G, \mathbf{k})$. This may account for the lack of attention paid to these rings so far. We shall give several examples showing that $\mathrm{gr} R(G, \mathbf{k})$ is far from trivial.

Proof. We make use of the *Adams operations* Ψ^k , which are defined in any λ -ring. When χ is the character of a representation, then $\Psi^k \chi(g) = \chi(g^k)$, for $g \in G$. So for $k = |G|$, we see that $\Psi^{|G|} \chi = \chi(1)$ (copies of the trivial representation). In particular $\Psi^{|G|} \chi$ depends only on the degree of χ , and so $\Psi^{|G|} x = 0$ for $x \in I$, the augmentation ideal. *A fortiori*, the operation $\Psi^{|G|}$ is zero on Γ^n .

However, we have for $n \geq 1$ and $x \in \Gamma^n$ the relation

$$\Psi^k x = k^n x \mod \Gamma^{n+1},$$

see Proposition III, 3.1 in [FL85]. The result follows. \square

COROLLARY 3.3 – *Let the number of irreducible representations of the finite group G over k be $c + 1$. Then for $n \geq 1$ the group Γ^n is isomorphic to \mathbf{Z}^c as an abelian group, and consequently the group $\mathrm{gr}^n R(G, \mathbf{k})$ is generated by c elements.*

Proof. The group $R(G, \mathbf{k})$ is isomorphic to \mathbf{Z}^{c+1} , so the result is certainly true for $\Gamma^1 = I$. Moreover, the fact that Γ^n / Γ^{n+1} is torsion indicates that Γ^{n+1} has the same rank as Γ^n . \square

Let us start giving concrete calculations.

PROPOSITION 3.4 – Suppose $G = C_N$ is cyclic of order N , and assume that \mathbf{k} is algebraically closed, of characteristic prime to N . Then

$$\mathrm{gr} R(G, \mathbf{k}) = \frac{\mathbf{Z}[c_1(\rho)]}{(Nc_1(\rho))},$$

for some 1-dimensional representation ρ .

In particular for each $n \geq 1$ we have $\mathrm{gr}^n R(G, \mathbf{k}) = \mathbf{Z}/N$, generated by $c_1(\rho)^n$. Thus the graded representation ring in this case is abstractly isomorphic to the ring $H^{2*}(G, \mathbf{Z})$.

Proof. The irreducible representations are $1, \rho, \rho^2, \dots, \rho^{n-1}$. We have $c_1(\rho^k) = kc_1(\rho)$ (Lemma 3.1). From the definitions, we see that $\mathrm{gr} R(G, \mathbf{k})$ is thus generated by $c_1(\rho)$, and from the relation $\rho^N = 1$ we see that $Nc_1(\rho) = 0$. We need to show that there are no further relations. So we consider an integer d such that $dc_1(\rho)^n = 0$, and we will show that N divides d . This will show that $\mathrm{gr}^n R(G, \mathbf{k})$ is no smaller than \mathbf{Z}/N .

It is an easy general fact that, when all the irreducible representations of G are 1-dimensional, then $\Gamma^n = I^n$, the n -th power of the augmentation ideal. Now, we have $R(G, \mathbf{k}) = \mathbf{Z}[\rho]/(\rho^N - 1)$, and it is easy to see that I is the ideal generated by $\rho - 1$, so that I^n is generated by $(\rho - 1)^n$.

Write $x = c_1(\rho) = \rho - 1$ for simplicity. The relation $dx^n = 0$ in Γ^n/Γ^{n+1} lifts to $dx^n = P(x)x^{n+1}$ in $R(G, \mathbf{k})$ for a polynomial P , and in turn we may write this in the form

$$dx^n = P(x)x^{n+1} + Q(x)[(1+x)^N - 1]$$

in $\mathbf{Z}[x]$. If $n > 1$ then we may look at the terms of degree 1 on each side, and deduce that $Q(0) = 0$. So we may divide the equation by x and obtain a similar one with n replaced by $n - 1$. So we go all the way down to $n = 1$. In this case

$$dx = P(x)x^2 + Q(x)[(1+x)^N - 1],$$

and by looking at the terms of degree 1 we see that $d = Q(0)N$, which was what we wanted. \square

Now let us see how changing the field k affects the results.

PROPOSITION 3.5 – Let $G = C_N$ be cyclic of order N , and let $\mathbf{k} = \mathbf{R}$. Then

(1) If N is odd, one has

$$\mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2 = \mathbf{F}_2,$$

concentrated in degree 0.

(2) If $N = 2m$ with m odd, then

$$\mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2 = \mathbf{F}_2[c_1(\varepsilon)],$$

for some 1-dimensional representation ε .

(3) If $N = 2m$ with m even, then

$$\mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2 = \frac{\mathbf{F}_2[c_1(\varepsilon), c_2(r)]}{(c_1(\varepsilon)^2)},$$

where ε is 1-dimensional, and r is 2-dimensional.

Proof. The case (1) follows from Lemma 3.2. Assume $N = 2m$. The case $m = 1$ was already considered in the previous Proposition, since $R(C_2, \mathbf{R}) = R(C_2, \mathbf{C})$, so we assume $m > 1$.

In this proof we work with characters rather than representations. The irreducible characters of G over \mathbf{C} are $1, \rho, \rho^2, \dots, \rho^{N-1}$ as above. Put $r_k = \rho^k + \rho^{-k}$ and $\varepsilon = \rho^m$; in particular $r_0 = 2$ (two copies of the trivial character) and $r_m = 2\varepsilon$.

The group G has $m+1$ irreducible characters, namely r_k for $1 \leq k \leq m-1$, together with ε and the trivial character. When talking about the characters r_k the indices will always be understood modulo N .

The relation $c_1(r) = c_1(\det(r))$ always hold (it follows from the axioms for Chern classes). Thus we see that $c_1(r_k) = 0$. Moreover one checks immediately that

$$r_k r_\ell = r_{k+\ell} + r_{k-\ell}.$$

We have $c_2(r_{k+\ell} + r_{k-\ell}) = c_2(r_{k+\ell}) + c_2(r_{k-\ell})$, while $c_2(r_k r_\ell) = 2(c_2(r_k) + c_2(r_\ell)) = 0$ (since we have tensored with \mathbf{F}_2). We draw

$$c_2(r_{k+\ell}) = c_2(r_{k-\ell}).$$

For $\ell = 1$ this shows that $c_2(r_k)$ depends only on the parity of k ; for k even we thus have $c_2(r_k) = c_2(r_0) = 0$, while for k odd we have $c_2(r_k) = c_2(r_1)$.

Now, we use the relation $\varepsilon r_1 = r_{m+1}$, which upon comparison of the second Chern classes gives

$$(*) \quad c_2(r_1) + c_1(\varepsilon)^2 = c_2(r_{m+1}).$$

Here we need to distinguish between cases (2) and (3).

If m is odd, then $m+1$ is even and $c_2(r_{m+1}) = 0$, so that equation (*) shows that $c_2(r_1) = c_1(\varepsilon)^2$. In this case we see that $\text{gr } R(G, \mathbf{R}) \otimes \mathbf{F}_2$ is generated by $c_1(\varepsilon)$. To show that there are no relations, consider the subgroup $C_2 \subset C_N$ and the restriction map

$$\text{gr } R(C_N, \mathbf{R}) \otimes \mathbf{F}_2 \longrightarrow \text{gr } R(C_2, \mathbf{R}) \otimes \mathbf{F}_2 = \mathbf{F}_2[c_1(\bar{\varepsilon})].$$

The equality on the right-hand side is the case $m = 1$ already considered. It is clear that the restriction map sends ε to $\bar{\varepsilon}$ (in obvious notation), and so also $c_1(\varepsilon)$ to $c_1(\bar{\varepsilon})$. The result follows.

Now consider the case when m is even, so $m+1$ is odd and equation (*) reads $c_1(\varepsilon)^2 = 0$. We see that $\text{gr } R(G, \mathbf{R}) \otimes \mathbf{F}_2$ is generated by $c_1(\varepsilon)$ and $c_2(r_1)$, subject to $c_1(\varepsilon)^2 = 0$, and we need to show that there are no further relations. We claim that $c_2(r_1)^n \neq 0$ for all n , and that $c_1(\varepsilon)c_2(r_1)^n \neq 0$ for all n , which will suffice. To prove the claim we consider the map

$$\text{gr } R(G, \mathbf{R}) \longrightarrow \text{gr } R(G, \mathbf{C}) = \frac{\mathbf{Z}[c_1(\rho)]}{(Nc_1(\rho))},$$

the equality coming from the previous Proposition. The complexification map sends r_1 to $\rho + \rho^{-1}$ and ε to ρ^m ; so it sends $c_1(\varepsilon)$ to $mc_1(\rho)$ and $c_2(\rho)$ to $-c_1(\rho)^2$. From this it is immediate that $c_2(r_1)^n$ is not zero in $\text{gr}^{2n} R(G, \mathbf{R}) \otimes \mathbf{F}_2$, while for $c_1(\varepsilon)c_2(r_1)^n$ we see that it is not zero at least in $\text{gr}^{2n+1} R(G, \mathbf{R})$; tensoring with \mathbf{F}_2 will not hurt though, for the relation $\varepsilon^2 = 1$ yields $2c_1(\varepsilon) = 0$, so that $\text{gr}^{2n+1} R(G, \mathbf{R})$ is 2-torsion anyway. \square

We see that over the field of real numbers, the ring $\text{gr } R(G, \mathbf{R})$ seems to be related to $H^*(G, \mathbf{F}_2)$, rather than $H^{2*}(G, \mathbf{Z})$. This connection will be strengthened by the “character” which we will now define.

3.3. The character. We think of the following map as a mod 2 version of the Chern character.

THEOREM 3.6 – *For any topological space X , there is a map of rings*

$$\omega: \text{gr } K(X) \longrightarrow \mathcal{W}^*(X)/\mathcal{J}_X.$$

Moreover $\omega(c_i(\rho)) = w_i(\rho)$.

The proof will occupy the rest of this section. Throughout, we write Γ^n for the n -th stage in the γ -filtration of the λ -ring $K(X)$.

LEMMA 3.7 – *The application*

$$w_{2^n-1} : \Gamma^n \longrightarrow H^{2^n-1}(X)$$

vanishes on Γ^{n+1} . Thus it induces a map

$$\mathrm{gr}^n K(X) \longrightarrow H^{2^n-1}(X),$$

and this map is a homomorphism.

Proof. First, consider a class in Γ^{n+1} of the form

$$\rho = (L_1 - 1) \cdots (L_{n+1} - 1),$$

where each L_i is a line bundle. Then $w_{2^n-1}(\rho) = 0$ by Theorem 2.1 (applied for $n+1$).

In general, we appeal again to the splitting principle. An element $\rho \in \Gamma^{n+1}$ may be written as a sum of elements of the form

$$\gamma^{k_1}(E_1 - \varepsilon(E_1)) \cdots \gamma^{k_s}(E_s - \varepsilon(E_s))$$

with $\sum k_i \geq n+1$. However we may find a space Y and a map $Y \rightarrow X$ such that all the vector bundles E_i involved in the expression of ρ split as sums of line bundles when pulled-back to Y ; and moreover it may be arranged that the induced map $H^*(X) \rightarrow H^*(Y)$ is injective.

To avoid multiple subscripts, let us work with a single vector bundle E , splitting up as a sum $E = L_1 + \cdots + L_{\varepsilon(E)}$ over Y . Then $\gamma^k(E - \varepsilon(E))$ is the k -th symmetric function in the elements $L_i - 1 = \gamma^1(L_i - 1)$. From this and the particular case just studied, it follows easily that $w_{2^n-1}(\rho) = 0 \in H^{2^n-1}(Y)$, and so this class is also zero in $H^{2^n-1}(X)$.

That w_{2^n-1} is a homomorphism is already true on Γ^n , and follows from the fact that all the elements in this group have vanishing Stiefel-Whitney classes in degrees less than 2^{n-1} . \square

To understand the map just defined, it is sufficient to indicate its effect on product of Chern classes: indeed Γ^n/Γ^{n+1} is generated by those, by definition.

LEMMA 3.8 – *When $\sum k_i = n$, we have*

$$w_{2^n-1}(c_{k_1}(E_1) \cdots c_{k_s}(E_s)) = \theta_n(w_{k_1}(E_1) \cdots w_{k_s}(E_s)).$$

Proof. Again we start with the case when each E_i is a line bundle. In this case $c_k(E_i) = 0$ for $k > 1$, while $c_1(E_i) = E_i - 1$; so it suffices to show that

$$w_{2^n-1}((E_1 - 1) \cdots (E_n - 1)) = \theta_n(w_1(E_1) \cdots w_1(E_n)),$$

which is the statement of Theorem 2.1.

Unsurprisingly, the general case follows from the splitting principle. Since Chern classes and Stiefel-Whitney classes behave in the same way when a vector bundle splits as a sum, the argument is easy, and will be omitted. \square

The proof of the Theorem is now easy. Given an element $\rho \in \Gamma^n/\Gamma^{n+1}$, the class $w^{2^n-1}(\rho)$ is well-defined by Lemma 3.7, and is of the form $\theta_n(x)$ for $x \in \mathcal{W}^n(X)$. So we may set $\omega(\rho) = x \in \mathcal{W}^n(X)/\mathcal{I}_X$. Lemma 3.8 proves both that ω is a homomorphism of rings, and that its values on Chern classes are as announced in the Theorem. This concludes the proof.

As a by-product of the proof, we have the following result. Part (1) is probably well-known, but it is just as easy (and more convenient for our readers) to establish it directly. Part (2) should be compared with Corollary 3.3.

LEMMA 3.9 – *Let G be a finite group.*

(1) *The ring $\mathcal{W}^*(G)$ is generated by Stiefel-Whitney classes of real representations of G .*

(2) *There exists a constant C such that*

$$\dim_{\mathbf{F}_2} \mathcal{W}^n(G)/\mathfrak{I}_G \leq C$$

for all $n \geq 0$.

Proof. We use Atiyah and Segal's completion Theorem (see [AS69], Theorem 7.1), which states that $K(BG)$ is the I -adic completion of $R(G, \mathbf{R})$, where I is the augmentation ideal. Under this identification, we see that any virtual vector bundle ρ over BG may be approximated by a virtual representation r up to an element in a high power of I . Since $I^n \subset \Gamma^n$, we know from Lemma 3.7 that by taking n large enough we can insure that $w_i(\rho) = w_i(r)$ in a convenient range. This proves (1).

Property (2) follows from (1) and Corollary 2.12 applied to BG , keeping in mind that G only has finitely many real representations. \square

3.4. Applications. Our applications will use the natural map

$$\mathrm{gr} R(G, \mathbf{R}) \longrightarrow \mathrm{gr} K(BG),$$

which, when composed with the character ω , induces the map

$$\mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2 \longrightarrow \mathcal{W}^*(G)/\mathfrak{I}_G.$$

We will still denote this map by ω .

EXAMPLE 3.10 – We start with a few examples for which the source and target of ω can be computed separately with relative ease (yet they are relevant to our applications to Milnor K -theory). The notation is as in Proposition 3.5. Let $G = C_N$ be a cyclic group. The cohomology ring $H^*(G, \mathbf{F}_2)$ is well-known, and admits the same description as $\mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2$ as in Proposition 3.5, except that Chern classes are to be replaced with Stiefel-Whitney classes. In particular $\mathcal{W}^*(G) = H^*(G)$.

When N is odd, the map ω is an isomorphism for uninteresting reasons (both rings being trivial). When $N = 2m$ with m odd, we have $H^*(G, \mathbf{F}_2) \cong H^*(C_2, \mathbf{F}_2)$, induced by the inclusion $C_2 \subset C_N$; it follows from Proposition 2.10 that $\mathfrak{I}_G = (0)$. As a result $\omega: \mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2 \rightarrow H^*(G)$ is again an isomorphism.

When $N = 2m$ with m even however, we shall see that ω is not an isomorphism, even though $\mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2$ and $H^*(G)$ are abstractly isomorphic. Let us compute \mathfrak{I}_G first. We have $Sq^1(w_2(r_1)) = w_1(r_1)w_2(r_1)$ by Wu's formula, and $w_1(r_1) = w_1(\det(r_1)) = 0$; as a result $Sq^1 w_1(\varepsilon)w_2(r_1) = 0$, and $w_1(\varepsilon)w_2(r_1) \in \mathfrak{I}_G$. In fact \mathfrak{I}_G is generated by this element. Indeed consider the two maps

$$H^*(G)/(w_1(\varepsilon)w_2(r_1)) \longrightarrow H^*(G)/\mathfrak{I}_G \longrightarrow H^*(C_2) = \mathbf{F}_2[w_1(\varepsilon)].$$

The first one is surjective, and we need to see that it is an isomorphism. This is trivially the case in odd degrees, both groups being zero; in degree $2n$, the group $H^{2n}(G)/(w_1(\varepsilon)w_2(r_1))$ is generated by $w_2(r_1)^n$. The second map is the restriction map induced by the inclusion $C_2 \subset G$, so it sends $w_2(r_1)^n$ to $w_1(\varepsilon)^{2n}$. Thus $w_2(r_1)^n \neq 0$ in $H^*(G)/\mathfrak{I}_G$, and our computation of \mathfrak{I}_G is complete.

The map

$$\omega: \mathrm{gr} R(G, \mathbf{R}) \otimes \mathbf{F}_2 \longrightarrow H^*(G)/\mathfrak{I}_G$$

has the form

$$\frac{\mathbf{F}_2[c_1(\varepsilon), c_2(r_1)]}{(c_1(\varepsilon)^2)} \longrightarrow \frac{\mathbf{F}_2[w_1(\varepsilon), w_2(r_1)]}{(w_1(\varepsilon)^2, w_1(\varepsilon)w_2(r_1))},$$

with $c_1(\varepsilon) \mapsto w_1(\varepsilon)$ and $c_2(r_1) \mapsto w_2(r_1)$, so its kernel is generated by $c_1(\varepsilon)c_2(r_1)$.

The character ω will help us compute the graded representation ring of elementary abelian 2-groups.

PROPOSITION 3.11 – *Let $G = (\mathbf{Z}/2)^r$. Over any field \mathbf{k} of characteristic different from 2, there are 1-dimensional representations $\varepsilon_1, \dots, \varepsilon_r$ such that the graded representation ring is*

$$\mathrm{gr} R(G, \mathbf{k}) \otimes \mathbf{F}_2 = \frac{\mathbf{F}_2[c_1(\varepsilon_1), \dots, c_1(\varepsilon_r)]}{(c_1(\varepsilon_i)^2 c_1(\varepsilon_j) + c_1(\varepsilon_i) c_1(\varepsilon_j)^2)}$$

for $1 \leq i, j \leq r$.

Proof. The representation ring $R(G, \mathbf{k})$ is the same over any field of characteristic $\neq 2$, so we may as well take $\mathbf{k} = \mathbf{R}$. We have $R(G) = \mathbf{Z}[\varepsilon_1, \dots, \varepsilon_r]/(\varepsilon_i^2 - 1)$, where each ε_i has dimension 1, so the graded representation ring is generated by the classes $c_1(\varepsilon_i)$.

Let $x_i = \varepsilon_i - 1$. The relation $\varepsilon_i^2 = 1$ shows that $x_i^2 = -2x_i$, so that $x_i^2 x_j = x_i x_j^2 = -2x_i x_j$. Given that $c_1(\varepsilon_i)$ is the image of x_i in Γ^1/Γ^2 , we certainly have the relation $c_1(\varepsilon_i)^2 c_1(\varepsilon_j) = c_1(\varepsilon_i) c_1(\varepsilon_j)^2$.

To prove that there are no more relations, we use the character ω , which maps the graded representation ring into $H^*(G)/\mathfrak{I}_G$. The latter is presented in Proposition 2.10, and we have $c_1(\varepsilon_i) \mapsto w_1(\varepsilon_i) = t_i$ in the notation of that Proposition. It is immediate that ω is an isomorphism, and the proof is complete. \square

There seems to be no elementary way (that is, not relying on the character) to prove this Proposition.

The example of elementary abelian groups is useful when studying larger groups, as we now show with the example of the dihedral group. Before stating the result, let us fix some notation. We write D_4 for the dihedral group of order 8. The representation ring $R(D_4, \mathbf{k})$ is the same over any field of characteristic $\neq 2$: there is a unique irreducible representation of dimension 2 which we call Δ , and four irreducible representation of dimension 1, say r_1, r_2 , and $r_3 = r_1 r_2 = \lambda^2(\Delta)$, together with the trivial one. The cohomology ring is given by

$$H^*(D_4) = \frac{\mathbf{F}_2[w_1(r_1), w_1(r_2), w_2(\Delta)]}{(w_1(r_1)w_1(r_2))} = \mathcal{W}^*(D_4).$$

(Here the representations are taken over \mathbf{R} of course.)

PROPOSITION 3.12 – *Over any field \mathbf{k} of characteristic $\neq 2$, the graded representation ring of the dihedral group is given by*

$$\mathrm{gr} R(D_4, \mathbf{k}) \otimes \mathbf{F}_2 = \frac{\mathbf{F}_2[c_1(r_1), c_1(r_2), c_2(\Delta)]}{(c_1(r_1)c_1(r_2), c_1(r_1)c_2(\Delta) + c_1(r_2)c_2(\Delta))}.$$

On the other hand, the ideal I_{D_4} is generated by $w_1(r_1)w_2(\Delta)$ and $w_1(r_2)w_2(\Delta)$. The kernel of the character ω is generated by $c_1(r_1)c_2(\Delta)$ and $c_1(r_2)c_2(\Delta)$.

Proof. First we show that the relations stated actually hold in the graded representation ring. The class $c_2(\Delta)$ is the image of $\gamma^2(\Delta - 2)$ in Γ^2/Γ^3 . By definition we have

$$\begin{aligned} \gamma^2(\Delta - 2) &= \lambda^2(\Delta - 1) \\ &= 1 - \lambda^1(\Delta) + \lambda^2(\Delta) \\ &= 1 - \Delta + r_1 r_2. \end{aligned}$$

On the other hand $c_1(r_i)$ is the image of $\gamma^1(r_i - 1) = r_i - 1$. We compute, using the relation $r_i\Delta = \Delta$, that

$$\begin{aligned}\gamma^2(\Delta - 2)\gamma^1(r_i - 1) &= r_1 + r_1 - r_1r_2 - 1 \\ &= -(r_1 - 1)(r_2 - 1) \\ &= -\gamma^1(r_1 - 1)\gamma^1(r_2 - 1).\end{aligned}$$

Thus we see that $\gamma^1(r_1 - 1)\gamma^1(r_2 - 1) \in \Gamma^3$, so $c_1(r_1)c_1(r_2) = 0$. On the other hand, we also observe that $\gamma^2(\Delta - 2)\gamma^1(r_i - 1)$ has the same expression for $i = 1$ and $i = 2$, so that $c_1(r_1)c_2(\Delta) = c_1(r_2)c_2(\Delta)$, as announced.

To show that there are no further relations, we study the restrictions to various subgroups. First, there are two copies of $C_2 \times C_2$ in D_4 , and the restriction map has the form

$$\mathrm{gr} R(D_4, \mathbf{k}) \otimes \mathbf{F}_2 \longrightarrow \mathrm{gr} R(C_2 \times C_2, \mathbf{k}) \otimes \mathbf{F}_2 = \frac{\mathbf{F}_2[a, b]}{(a^2b + ab^2)},$$

where the equality comes from the previous Proposition. For one copy of $C_2 \times C_2$, with a judicious choice of coordinates, we have $c_1(r_1) \mapsto a + b$, $c_1(r_2) \mapsto 0$, and $c_2(\Delta) \mapsto ab$. What is more, using a different subgroup, we obtain a restriction map with the roles of r_1 and r_2 exchanged. This is already enough to see that the elements $c_1(r_1)^{2n}$, $c_1(r_2)^{2n}$ and Δ^n are linearly independent in $\mathrm{gr}^{2n} R(D_4, \mathbf{k}) \otimes \mathbf{F}_2$.

There is also a copy of C_4 in D_4 , and this time the restriction map looks like

$$\mathrm{gr} R(D_4, \mathbf{k}) \otimes \mathbf{F}_2 \longrightarrow \mathrm{gr} R(C_4, \mathbf{k}) \otimes \mathbf{F}_2 = \frac{\mathbf{F}_2[x, y]}{(x^2)},$$

where the equality was proved in Example 3.10. Under this map we have $c_1(r_1) \mapsto x$, $c_1(r_2) \mapsto x$, and $c_2(\Delta) \mapsto y$. The three restriction maps combined allow us to see that $c_1(r_1)^{2n+1}$, $c_1(r_2)^{2n+1}$, and $c_1(r_1)\Delta^n$ are linearly independent in $\mathrm{gr}^{2n+1} R(D_4, \mathbf{k})$. It follows that the relations are precisely as stated.

To compute the ideal I_{D_4} , we use Wu's formula again, which gives $Sq^1w_2(\Delta) = w_1(\Delta)w_2(\Delta) = w_1(r_1r_2)w_2(\Delta) = (w_1(r_1) + w_1(r_2))w_2(\Delta)$. As a result

$$Sq^1(w_1(r_1)w_2(\Delta)) = w_1(r_1)^2w_2(\Delta) + w_1(r_1)w_2(\Delta) + w_1(r_1)w_1(r_2)w_2(\Delta) = 0.$$

It follows that $w_1(r_1)w_2(\Delta) \in I_{D_4}$, and likewise for $w_1(r_2)w_2(\Delta)$. To show that there are no further generators needed for I_{D_4} , we study the restrictions to the above subgroups. This is left to the reader. \square

4. APPLICATIONS TO MILNOR K -THEORY

4.1. Technicalities on profinite groups. When dealing with Galois theory, we shall encounter profinite groups. Let us indicate our conventions.

Let G be profinite. A representation of G over \mathbf{k} , by convention, means a finite-dimensional \mathbf{k} -vector space with an action of G which factors through a quotient G/U where U is open. Such a U is closed and of finite index, so that G/U is finite. It follows that the category of representations of G is semi-simple.

The Grothendieck group of this category is what we call $R(G, \mathbf{k})$. As an abelian group, it is free with a basis given by the irreducible representations. The maps $R(G/U, \mathbf{k}) \rightarrow R(G, \mathbf{k})$ are thus injective, when U is as above, and it follows easily that

$$R(G, \mathbf{k}) = \mathrm{colim}_U R(G/U, \mathbf{k}).$$

The colimit is taken over a directed set, since $U \cap V$ is open when U and V are; so we can think of it essentially as a union. It is clear that $R(G, \mathbf{k})$ is a λ -ring.

The ‘‘line elements’’ in $R(G, \mathbf{k})$, as in [FL85], are the 1-dimensional representations, which form the group $\mathrm{Hom}(G, k^\times)$ where continuous homomorphisms are

meant (using the discrete topology of \mathbf{k}^\times). Lemma 3.1 applies to profinite groups with the same proof.

4.2. Milnor K -theory and the graded representation ring. Let us briefly recall the definition of mod 2 Milnor K -theory (using the notation which is classically employed for Milnor K -theory itself). Let F be any field. First one defines $k_1(F)$ to be the \mathbf{F}_2 -vector space $F^\times/(F^\times)^2$, written additively, and the letter ℓ is used to denote the identity

$$\ell: F^\times/(F^\times)^2 \longrightarrow k_1(F),$$

so that $\ell(ab) = \ell(a) + \ell(b)$. Then one considers the tensor algebra $T^*(k_1(F))$, and the ideal M generated by the Matsumoto relations, that is $\ell(a)\ell(b) = 0$ whenever $a+b = 1$. The algebra $k_*(F) = T^*(k_1(F))/M$, which is commutative, is the mod 2 Milnor K -theory of F .

THEOREM 4.1 – *Let F be any field, and let \mathbf{k} be any field of characteristic different from 2, not containing $\sqrt{-1}$. Let \bar{F} be the separable closure of F , and let $G = \text{Gal}(\bar{F}/F)$ be the absolute Galois group of F . Then there is a map*

$$\rho: k_*(F) \longrightarrow \text{gr } R(G, \mathbf{k}) \otimes \mathbf{F}_2.$$

If \mathbf{k} possesses an embedding into \mathbf{R} , then there is a commutative square

$$\begin{array}{ccc} k_*(F) & \xrightarrow{\rho} & \text{gr } R(G, \mathbf{k}) \otimes \mathbf{F}_2 \\ h_F \downarrow & & \downarrow \omega \\ H^*(G) & \longrightarrow & H^*(G)/\mathfrak{I}_G. \end{array}$$

Here the map h_F is the one originally defined by Milnor. This map is an isomorphism, as the Milnor conjecture, now a theorem by Voevodsky, states. In particular $H^*(G)$ is generated by 1-dimensional classes, and thus by Stiefel-Whitney classes, so that $H^*(G) = \mathcal{W}^*(G)$. In any case it is trivially the case that h_F takes its values in $\mathcal{W}^*(G)$, even without assuming knowledge of the Voevodsky theorem.

Proof. We begin by defining a map

$$\tilde{\rho}: F^\times/(F^\times)^2 \longrightarrow \text{Hom}(G, k^\times).$$

If $a \in F^\times$, we consider the field extension $F[\sqrt{a}]$ (within the fixed separable closure \bar{F}). Then for $\sigma \in G$, we have $\sigma(\sqrt{a})/\sqrt{a} = \pm 1$. Thus we define a continuous homomorphism $\tilde{\rho}(a): G \rightarrow k^\times$ by setting $\tilde{\rho}(a)(\sigma) = \sigma(\sqrt{a})/\sqrt{a}$. It is immediate that $\tilde{\rho}$ is a homomorphism, and depends only on the class of a modulo squares.

Since $\text{Hom}(G, k^\times)$ is none other than the group of 1-dimensional representations of G over \mathbf{k} , under the tensor product operation, we see from Lemma 3.1 that we may in fact define a map

$$\rho: k_1(F) \longrightarrow \text{gr}^1 R(G, \mathbf{k}) \otimes \mathbf{F}_2$$

by $\rho = c_1 \circ \tilde{\rho} \circ \ell^{-1}$ (here c_1 is the first Chern class).

This extends to a map $T^*(k_1(F)) \rightarrow \text{gr } R(G, \mathbf{k}) \otimes \mathbf{F}_2$, and to factor it into a map on $k_*(F)$ we need to show that the elements $\ell(a)\ell(b)$ are sent to 0 when $a+b = 1$. Let us use an elementary result from Galois theory: when $a+b = 1$, and when a and b are linearly independent in $F^\times/(F^\times)^2$ (over \mathbf{F}_2), then the fields $F[\sqrt{a}]$ and $F[\sqrt{b}]$ are both contained in a field E such that E/F is Galois with $\text{Gal}(E/F) = D_4$, the dihedral group of order 8. Moreover, the homomorphisms $\tilde{\rho}(a)$ and $\tilde{\rho}(b)$ factor through D_4 , and as representations of this group they correspond to r_1 and r_2 in the notation of Proposition 3.12. However this very Proposition states that

$$c_1(r_1)c_1(r_2) = 0 = \rho(\ell(a))\rho(\ell(b)).$$

We also need to take care of the case $a = b \neq 0$ in the vector space $F^\times/(F^\times)^2$. Again, elementary Galois theory tells us that in this situation, the field $F[\sqrt{a}]$ is contained in a field E such that E/F is Galois with Galois group $\mathbf{Z}/4$. The hypotheses on \mathbf{k} guarantee that $R(\mathbf{Z}/4, \mathbf{k})$ is the same as $R(\mathbf{Z}/4, \mathbf{R})$ (if \mathbf{k} were to contain $\sqrt{-1}$, the ring $R(\mathbf{Z}/4, \mathbf{k})$ would be the same as $R(\mathbf{Z}/4, \mathbf{C})$ and the Theorem would not hold). Moreover $\tilde{\rho}(a)$ factors through $\mathbf{Z}/4$ as the representation ε , in the notation of Proposition 3.5. This Proposition states that

$$c_1(\varepsilon)^2 = 0 = \rho(\ell(a))^2.$$

Thus ρ factors through $k_*(F)$.

The commutativity of the square follows from the property $\omega(c_1(r)) = w_1(r)$ for any representation r . Indeed, Milnor's map sends $\ell(a)$ to $w_1(\tilde{\rho}(a))$ (when $\mathbf{k} = \mathbf{R}$). \square

Of course one may wonder whether the map ρ is an isomorphism, just like h_F is, and for what choices of \mathbf{k} . In general, this is a hard question, and we will study a certain variant which lends itself to computation more easily. Assume that F has characteristic $\neq 2$. Following [MS96], let F_q be the quadratic closure of F (the compositum within \bar{F} of all finite extensions of F whose degree is a power of 2). Let $Q = \text{Gal}(F_q/F)$, which is a quotient of $G = \text{Gal}(\bar{F}/F)$. Then define

$$\mathcal{G} = Q/Q^4[Q^2, Q].$$

This group is called the W -group of F because of its relation with the Witt ring. We are interested in \mathcal{G} because it is much easier to deal with than G itself; for example when $F^\times/(F^\times)^2$ is finite then \mathcal{G} is also finite. However, the cohomological information of F is preserved, since

$$H^*(G) = H^*(\mathcal{G})_{dec}.$$

(See [AKM99], Theorem 3.14.) We then think of the following Theorem as an amendment to Theorem 4.1.

THEOREM 4.2 – *Let F and \mathbf{k} be fields of characteristic different from 2, with \mathbf{k} not containing $\sqrt{-1}$. Let \mathcal{G} be the W -group of F . Then there is a map*

$$\rho: k_*(F) \longrightarrow (\text{gr } R(\mathcal{G}, \mathbf{k}) \otimes \mathbf{F}_2)_{dec}.$$

If \mathbf{k} possesses an embedding into \mathbf{R} , then there is a commutative square

$$\begin{array}{ccc} k_*(F) & \xrightarrow{\rho} & (\text{gr } R(\mathcal{G}, \mathbf{k}) \otimes \mathbf{F}_2)_{dec} \\ h_F \downarrow & & \downarrow \omega \\ H^*(\mathcal{G})_{dec} & \longrightarrow & H^*(\mathcal{G})_{dec}/\mathcal{I}_{\mathcal{G}}. \end{array}$$

Proof. Since the extension of F corresponding to \mathcal{G} contains all the extensions with Galois group D_4 ([MS96], Corollary 2.18), the same proof works *mutatis mutandis*. \square

We are already capable of proving that there are very few possibilities for \mathbf{k} :

LEMMA 4.3 – *Let \mathbf{k} have characteristic 0.*

- *Either \mathbf{k} contains $\sqrt{-1}$, and the inclusion $\mathbf{Q}(\sqrt{-1}) \rightarrow k$ induces an isomorphism $R(\mathcal{G}, \mathbf{Q}(\sqrt{-1})) = R(\mathcal{G}, \mathbf{k})$; in particular one has $R(\mathcal{G}, \mathbf{k}) = R(\mathcal{G}, \mathbf{C})$.*
- *Or, \mathbf{k} does not contain $\sqrt{-1}$, and the inclusion $\mathbf{Q} \rightarrow k$ induces an isomorphism $R(\mathcal{G}, \mathbf{Q}) = R(\mathcal{G}, \mathbf{k})$; in particular one has $R(\mathcal{G}, \mathbf{k}) = R(\mathcal{G}, \mathbf{R})$.*

Proof. Every element in \mathcal{G} has order dividing 4. \square

So we are essentially left with the cases $\mathbf{k} = \mathbf{C}$ and $\mathbf{k} = \mathbf{R}$. We have already dismissed the choice $\mathbf{k} = \mathbf{C}$.

LEMMA 4.4 – *When $\mathbf{k} = \mathbf{Q}$ or \mathbf{R} , the map*

$$\rho: k_*(F) \longrightarrow (\mathrm{gr} R(\mathcal{G}, \mathbf{k}) \otimes \mathbf{F}_2)_{dec}$$

is always surjective, and is an isomorphism in degrees 1 and 2.

Proof. The map ρ is an isomorphism in degree 1 by choice of \mathbf{k} , as already alluded to (cf Lemma 3.1). The target of this map is generated by elements of degree 1 by definition, so ρ is surjective.

In degree 2, we consider the commutative square of Theorem 4.2. The map h_F is injective (in degree 2 this is a theorem of Merkurjev's, which is used in the general proof of Voevodsky-Rost). The map $H^2(\mathcal{G})_{dec} \rightarrow H^2(\mathcal{G})_{dec}/\mathfrak{I}_{\mathcal{G}}$ is also injective, since θ_2 is the identity. It follows that ρ is injective in degree 2. \square

4.3. Examples. We fix the choice $\mathbf{k} = \mathbf{R}$ for definiteness. We shall give a collection of examples of fields F , assumed to be of characteristic $\neq 2$, for which the map

$$\rho: k_*(F) \longrightarrow (\mathrm{gr} R(\mathcal{G}, \mathbf{R}) \otimes \mathbf{F}_2)_{dec}$$

is an isomorphism. In each case this will follow either directly from Lemma 4.4 or from the fact that the W -group \mathcal{G} is a finite group whose graded representation ring we have been able to compute. Note that there is yet no example of field F such that ρ is not an isomorphism.

4.3.1. F finite. In this case the group \mathcal{G} is $\mathbf{Z}/4$, so that both the Galois cohomology and the Milnor K -theory of F are concentrated in degrees ≤ 2 ; the same can thus be said of $(\mathrm{gr} R(\mathcal{G}, \mathbf{R}) \otimes \mathbf{F}_2)_{dec}$, from the surjectivity statement in Lemma 4.4. The same Lemma shows that ρ is an isomorphism. This is consistent with Proposition 3.5.

4.3.2. F real closed. In this case $\mathcal{G} = \mathbf{Z}/2$, so $H^*(\mathcal{G}) = \mathbf{F}_2[t]$ with t of degree 1. The map ρ is clearly an isomorphism, by Lemma 4.4 and Proposition 3.5 combined.

4.3.3. F a local field. In this case $k_*(F)$ is again concentrated in degrees ≤ 2 , so ρ is an isomorphism.

4.3.4. F a global field. We use the commutative diagram

$$\begin{array}{ccc} k_*(F) & \xrightarrow{\rho} & (\mathrm{gr} R(\mathcal{G}, \mathbf{R}) \otimes \mathbf{F}_2)_{dec} \\ \downarrow & & \downarrow \\ \bigoplus_v k_*(F_v) & \xrightarrow{\oplus \rho_v} & \bigoplus_v (\mathrm{gr} R(\mathcal{G}_v, \mathbf{R}) \otimes \mathbf{F}_2)_{dec} \end{array}$$

Here the direct sums extend over all the real completions F_v of the field F , while \mathcal{G}_v is the W -group of F_v , and ρ_v has an obvious meaning. The vertical map on the left is an isomorphism in degrees ≥ 3 by Tate (see [Mil70], Appendix), and the maps ρ_v are isomorphisms by the real case already considered, so ρ is injective, as well as surjective, in those degrees. Finally ρ is an isomorphism in all degrees in this case, too.

4.3.5. *Some C -fields.* When F is a C -field of level 1, the W -group \mathcal{G} is $\prod_{i \in I} \mathbf{Z}/4$, where I is a (possibly infinite) basis of $F^\times / (F^\times)^2$. When I has order n , then the ring $H^*(\mathcal{G})_{dec}$ is an exterior algebra on n generators in degree 1, so it is concentrated in degrees $\leq n$. For $n \leq 2$, it follows that ρ is an isomorphism. For $n = 3$, a computer calculation which we will not reproduce here shows that ρ is again an isomorphism. It remains an open problem to compute the graded representation ring of $(\mathbf{Z}/4)^n$, and the character ω is of no help here: one can check that $I_{(\mathbf{Z}/4)^n} = H^{\geq 3}((\mathbf{Z}/4)^n)$.

4.3.6. *Any field whose W -group is D_4 .* This is the case of the field $F = \mathbf{R}((u))((v))$ for example. From Proposition 3.12, it follows that ρ is an isomorphism.

4.3.7. *Any field with a universal W -group.* Given any set I , there is a universal W -group which we will write here \mathcal{G}_I . When F is a field such that $F^\times / (F^\times)^2$ has a basis in bijection with I , then its W -group \mathcal{G} is a quotient of \mathcal{G}_I . It may happen that $\mathcal{G} = \mathcal{G}_I$ (see [GM97] for examples). In this case, from the fact that $H^2(\mathcal{G}_I) = 0$, we see that the Galois cohomology is concentrated in degrees ≤ 1 , so ρ is certainly an isomorphism.

4.3.8. *Any field for which $\ell(-1)$ is not a zero divisor.* To treat this case, we begin by establishing a simple formula for the action of the operations θ_n in the case of Galois cohomology. The formula was anticipated in the Introduction.

LEMMA 4.5 – *Let G be the absolute Galois group of a field F , and let $x \in H^n(G)$. Then $\theta_n(x) = \ell(-1)^{2^{n-1}-n}x$.*

Proof. Since $H^*(G)$ is generated by elements of degree 1, it is enough to prove this for $x = t_1 t_2 \cdots t_n$ with $t_i \in H^1(G)$. In this case the value of $\theta_n(t_1 \cdots t_n)$ is given by Lemma 2.5. However, in Galois cohomology one has $t^2 = \ell(-1)t$ for any t of degree 1. It follows that there exists a constant c_n , depending only on n , such that $\theta_n(x) = c_n \ell(-1)^{2^{n-1}-n}x$ for any x of this form (namely, c_n is the number of terms in the sum appearing in the statement of Lemma 2.5, reduced mod 2).

It remains to see that $c_n \neq 0$. Indeed if it were 0, then one would have $\theta_n(x) = 0$ for any $x \in H^n(G)$, regardless of G . However the example of $\mathbf{Z}/2$ (which is the absolute Galois group of \mathbf{R}) shows that $\theta_n x$ can be non-zero, since Proposition 2.10 establishes that $\mathfrak{I}_{\mathbf{Z}/2} = (0)$. \square

The commutative square of Theorem 4.2 then shows clearly that ρ is an isomorphism when $\ell(-1)$ is not a zero divisor.

REFERENCES

- [AKM99] Alejandro Adem, Dikran B. Karagueuzian, and Ján Mináč. On the cohomology of Galois groups determined by Witt rings. *Adv. Math.*, 148(1):105–160, 1999.
- [AS69] M. F. Atiyah and G. B. Segal. Equivariant K -theory and completion. *J. Differential Geometry*, 3:1–18, 1969.
- [AT69] M. F. Atiyah and D. O. Tall. Group representations, λ -rings and the J -homomorphism. *Topology*, 8:253–297, 1969.
- [FL85] William Fulton and Serge Lang. *Riemann-Roch algebra*, volume 277 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.
- [GM97] Wenfeng Gao and Ján Mináč. Milnor’s conjecture and Galois theory. I. In *Algebraic K-theory (Toronto, ON, 1996)*, volume 16 of *Fields Inst. Commun.*, pages 95–110. Amer. Math. Soc., Providence, RI, 1997.
- [Kum75] Ernst Eduard Kummer. *Collected papers*. Springer-Verlag, Berlin, 1975. Volume I: Contributions to number theory, Edited and with an introduction by André Weil.
- [Mil58] John Milnor. The Steenrod algebra and its dual. *Ann. of Math. (2)*, 67:150–171, 1958.
- [Mil70] John Milnor. Algebraic K -theory and quadratic forms. *Invent. Math.*, 9:318–344, 1969/1970.

- [MS74] John W. Milnor and James D. Stasheff. *Characteristic classes*. Princeton University Press, Princeton, N. J., 1974. Annals of Mathematics Studies, No. 76.
- [MS96] Ján Mináč and Michel Spira. Witt rings and Galois groups. *Ann. of Math. (2)*, 144(1):35–60, 1996.
- [OVV07] D. Orlov, A. Vishik, and V. Voevodsky. An exact sequence for $K_*^M/2$ with applications to quadratic forms. *Ann. of Math. (2)*, 165(1):1–13, 2007.
- [Voe03a] Vladimir Voevodsky. Motivic cohomology with $\mathbf{Z}/2$ -coefficients. *Publ. Math. Inst. Hautes Études Sci.*, (98):59–104, 2003.
- [Voe03b] Vladimir Voevodsky. Reduced power operations in motivic cohomology. *Publ. Math. Inst. Hautes Études Sci.*, (98):1–57, 2003.

PIERRE GUILLOT, UNIVERSITÉ DE STRASBOURG, INSTITUT DE RECHERCHE MATHÉMATIQUE
 AVANCÉE, 7 RUE RENÉ DESCARTES, 67084 STRASBOURG, FRANCE
E-mail address: guillot@math.unistra.fr

JÁN MINÁČ, DEPARTMENT OF MATHEMATICS, MIDDLESEX COLLEGE, THE UNIVERSITY OF
 WESTERN ONTARIO, LONDON, ONTARIO, CANADA, N6A 5B7
E-mail address: minac@uwo.ca